Digital Upgrades of the Non-Safety Related NSSS Control Systems at Byron and Braidwood Stations

John Connelly
Engineering Manager – Capital Projects
Exelon Generation Company

May 20, 2015

Agenda

- Introductions and Opening Remarks
- Meeting Purpose
- Problem Statement
- Exelon and Industry Perspective
- Project Scope
- Modernization Strategy
- Governing Design Principles
- Conclusions

Meeting Purpose

- Outline the Exelon project for upgrading the Non-Safety-Related (NSR) NSSS Control Systems at Byron and Braidwood Stations

- Engage the Staff in an open and transparent dialog regarding the modification scope and the licensing basis that supports performing this upgrade in accordance with the well vetted 10 CFR 50.59 process
  - While interface protocols exist for vetting Safety-Related digital modifications (i.e., ISG-06), there is no published corollary process for NSR digital modifications conducted under the 50.59 process

- Obtain staff feedback on Exelon's modernization initiative and identify potential technical and regulatory areas of concern that warrant additional discussion

Problem Statement

- The NSR NSSS control systems at Byron and Braidwood are original construction and have been in service for more than 30 years
- The NSSS control systems in their current form lack adequate redundancy, are not sufficiently fault tolerant and there are no practical means to address this inherent architectural limitation using analog technology
- Systems have been properly maintained and upgraded in-kind to the extent practical; however systems are nearing the end of their practical service life
- With planned License Extensions, the systems will need to remain in service and reliable for up to 33 additional years*
- The primary project objective is to improve Equipment Reliability and reduce exposure to plant transients and initiating events thereby improving margins of safety

*Byron Units 1&2 from 2024 & 2026 to 2044 & 2046 respectively
*Braidwood Units 1&2 from 2026 & 2027 to 2046 & 2047 respectively

Problem Statement

Historical System Performance – RX Trip Data

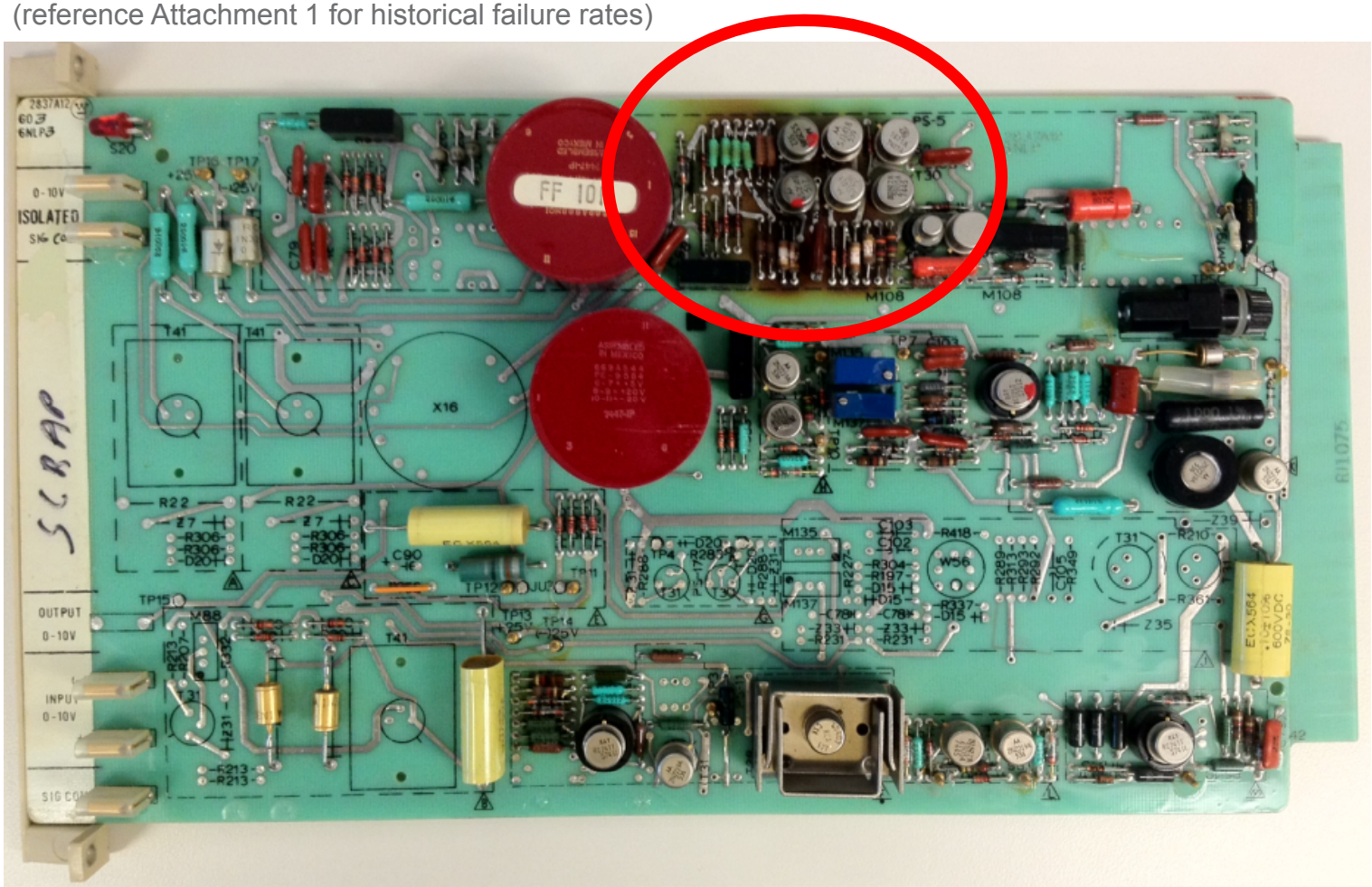
- From 2000 to 2013 Byron and Braidwood have experienced a total of 21 RX trips
- 10 of those events (47%) were attributed to failures of the systems we intend to modernize
- 8 of those events (38%) would have been prevented by the strategies proposed. The remaining 2 were addressed in 2005-2007 through similar modifications (DEH upgrade project)
- This event rate translates into 0.62 RX trips / year and would be expected to gradually increase over time as systems continue to age
- System performance analysis did not consider successfully mitigated transients – examples of excluded events:
  - Deselecting faulted instrument channels
  - Taking manual control of faulted control systems
  - Failures of the feedpump control system mitigated by promptly reducing turbine load or “fast starting” the MDFWP (or both)
  - Dropped control rod events mitigated by reducing RX power and retrieving dropped rod(s)

Problem Statement

Circuit Card Service Life

The service life of 7300 circuit card is constrained principally by the PS-5 DC-DC converter circuit common to nearly all cards

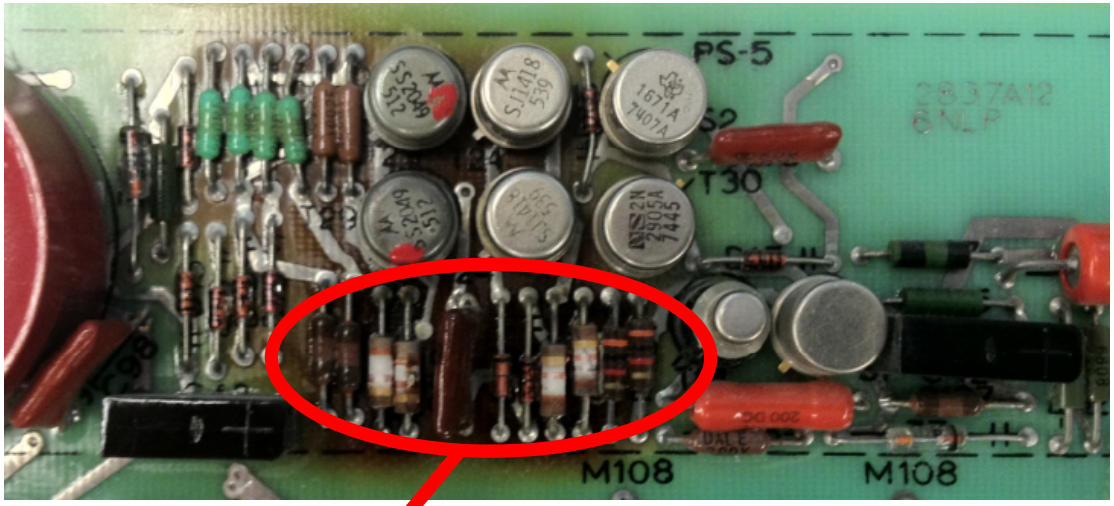
(reference Attachment 1 for historical failure rates)



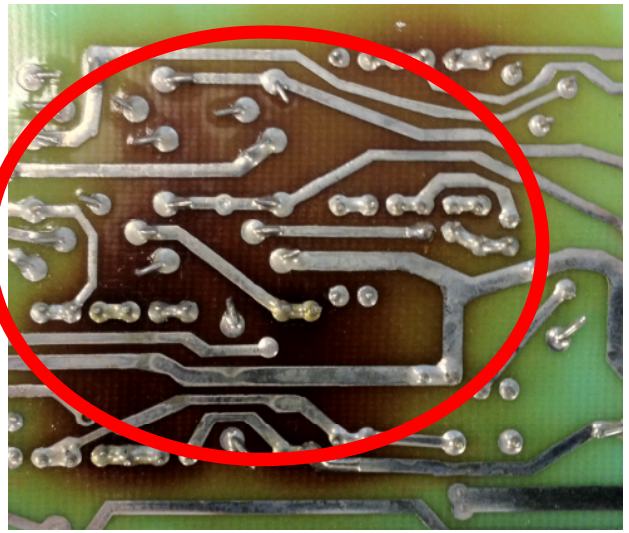
Exelon Generation

Problem Statement

Typical age related degradation of PS-5



Charred diodes and resistors



Heat damage to trace side of PCB

Exelon and Industry Perspective

- Our shared goal is safe and reliable operation
- The industry position is that digital modernization initiatives can and should be performed within the confines of the well vetted 50.59 process where supported by the appropriate technical basis and rigorous analysis
- Modernization efforts are imperative to addressing key plant performance issues:
  - Reduction of initiating events
  - Improved Equipment Reliability
  - Management of component obsolescence

Project Scope

Conceptual Design Study

- In 2013, Exelon conducted a detailed Conceptual Design Study of the Byron / Braidwood I&C Long Term Asset Management (LTAM) strategy

- The project team included a broad range of stakeholders:
  - Site System Engineers
  - Site Design Engineers
  - Corporate Engineering
  - Site and Corporate Training representatives
  - Information Technology
  - Cyber Security
  - Corporate Licensing
  - Project Management
  - Executive Leadership
  - Contracted Subject Matter Experts
  - Westinghouse
  - Architect / Engineers
  - Installers

- The results of the conceptual design study form the basis for today's presentation

Project Scope

The systems to be modernized are:

- NSR NSSS/BOP Process I&C System (Westinghouse 7300)
- Turbine Driven Feedwater Pump Speed Control (TDFWPSC)
- Rod Control System Logic Cabinets

Modernization Strategy

Exelon Generation®

Modernization Strategy

Westinghouse 7300 System Architecture Overview

Though often thought of as a single entity, the Westinghouse 7300 Process I&C System is, in reality, two largely separate but interconnected systems:

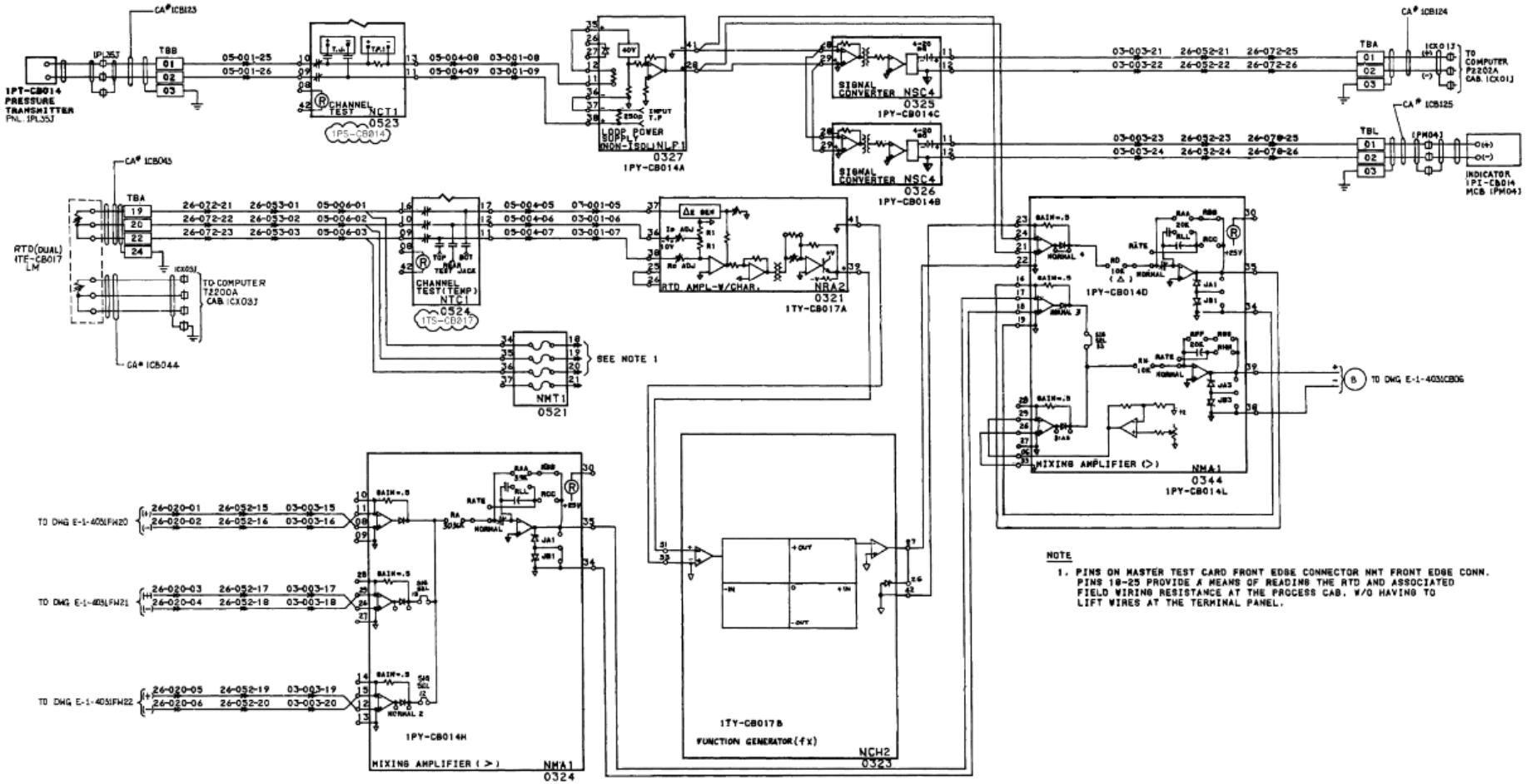
- **Reactor Protection System (RPS)**
  - Safety Related
  - Monitors key plant process parameters
  - Outputs feed Solid State Protection System (SSPS) logic to generate ESF actuations
  - Provides key process indications to MCR
  - Four fully independent protection channels
  - Inherently redundant
  - ~740 circuit cards per unit in the Reactor Protection System
  - NOT an element of the modernization initiative

- **NSSS and BOP Control Systems**
  - Non-Safety Related
  - Receives isolated outputs from the RPS (S/G NR Level, Delta-T…) which are used to control plant processes
  - Receives inputs from a wide variety of non-safety related field sensors
  - Generates process control outputs (FWP speed, FWRV, RY Press…)
  - Effectively no redundancy or inherent fault tolerance
  - ~1100 circuit cards per unit in BOP control system

- **Nearly all major plant systems either interface with 7300 or are directly controlled by it**

Modernization Strategy

Current Architecture Example *(FWP NPSH - partial)*



Exelon Generation

Modernization Strategy

- Migrate the NSR 7300 Process I&C control systems (NSSS and BOP) to a standard implementation of the Ovation™ Distributed Control System (DCS) – 11 control segments in total:
  - Consistent with control system architecture of AP-1000 new-builds
  - Installed domestically at McGuire and Catawba
  - Installed internationally at Almaraz, Kozloduy, Ringhals, Shin Kori and Shin Wolsong (et al)
- Migrate the existing NSR Rod Control Logic cabinet to Ovation™ DCS with functionally segregated controller pairs
- Migrate the TDFWP controls and coordinate with the NSSS upgrade through the addition of functionally segregated Ovation™ DCS controller pairs
- Address peripheral obsolescence issues as an element of the larger migration strategy
  - Obsolete M/A stations
  - Obsolete electro-mechanical rod bank step counters
  - Obsolete DEH workstations

Modernization Strategy

Turbine Driven Feedwater Pump (TDFWP)

- The existing TDFWP control system has a large population of SPV's including:
  - Circuit cards
  - Relays
  - Speed Setter Motor Operated Potentiometers (SS-MOP's)
  - LVDT's
  - Tach-Paks
  - Mechanical Overspeed System
  - EH fluid components
  - Oil pumps / accumulators
  - Pressure switches
  - Solenoid valves
  - Power supplies
  - 7300 cards that provide the speed reference demand signals
- Byron and Braidwood are one of the few plants in the industry that have maintained the original analog control systems – industry peers have implemented digital controls and in many cases are on the second generation of digital upgrades
- Interim coping strategy are in place (principally reverse engineering of analog components) but these strategies have not been without issue and do nothing to eliminate the SPV's inherent in the original design

Modernization Strategy

Rod Control System

- The existing RD Logic Cabinet is original construction and is nearing the end of practical service life
- The system design is not fault tolerant and lacks inherent redundancy
- The existing RD system is exceptionally complex and bench strength is very limited
- OPEX identifies 28 Reactor Trips due to failures of the Westinghouse RD system between 2000 and 2010
- Next Generation circuit cards are available; however, this pathway does not address the inherent limitations of the system design, its complexity or limited bench strength
  - The limited Operating Experience (OPEX) is mixed
  - Farley installed next-gen circuit cards and has experienced 2 reactor trips from early card failures

Modernization Strategy

Collateral Benefits

- Hardware component count is reduced by ~80% – hardware that does not exist is hardware that cannot fail
- Eliminates existing control system SPV's
- Enables the application of advanced control strategies that cannot be achieved with existing architecture (mode dependent SGWLC, signal arbitration, automated fault deselect…)
- Circuit card calibrations are completely eliminated freeing substantial maintenance resources to focus on other plant performance improvements
- Vastly expanded diagnostics, performance monitoring and access to plant data
- Obsolete M/A Stations are replaced with Small Loop Interface Modules (SLIM's) which provides an additional layer of defense completely independent of controllers
- Obsolete electro-mechanical rod bank counters are replaced with LCD equivalents
- Positions sites for safe and reliable operation through end of plant life
- Creates opportunities for smart field instrumentation which provides plant performance insights not currently available

Governing Design Principles

Exelon Generation®

Governing Design Principles

The conceptual design study followed 7 general design principles:

Technical

1. Selected platform must be well vetted with a demonstrated history of reliable operation
2. Software development processes should take maximum advantage of well vetted and recognized industry standards
3. Verification and Validation (V&V) protocols executed consistent with well vetted and recognized industry standards
4. A CCF susceptibility analysis will be performed and, for any CCF that cannot be prevented, a CCF coping analysis will be performed to determine the plant level effects. Appropriate mitigation strategies will be applied as necessary

Licensing

5. Appropriate functional segregation must be maintained to remain within the boundaries of the UFSAR
6. Design should not necessitate changes to existing Technical Specifications
7. Software design (system behaviors) to remain consistent with existing licensing basis

Technical Principle - Platform OPEX

- The Ovation™ Digital Control System is a well vetted and mature platform deployed worldwide in nuclear, fossil and critical infrastructure applications
- There are currently more than 100 Ovation™ systems deployed in a variety of nuclear applications worldwide with a combined total of 373 years of operating experience
- There are currently more than 1400 Ovation™ systems deployed in a variety of non nuclear applications worldwide with a combined total of 9,058 years of operating experience
- The industry average failure rate for 7300 circuit cards is 0.7% per year – Exelon has been able to maintain a failure rate of 0.4% per year by investing heavily in preemptive circuit card replacements – Historical data for Ovation yields a failure rate of 0.001%
- Largely identical applications are currently in service both domestically and internationally
  - Installed domestically at both McGuire and Catawba under 50.59
  - Installed internationally at Almaraz, Kozloduy, Ringhals, Shin Kori and Shin Wolsong
- Architecture is consistent with control system architecture of the AP-1000 new-builds

Licensing Principle - Functional Segregation

- *The plant design basis is maintained* by utilizing the requirements from the original plant design documents and applying these to the new control system design:
  - WEC System Functional Requirements Specification
  - WEC System Process Block Diagrams
  - WEC Precautions, Limitations and Setpoint Document

Resulting Design = Technical Principles + Licensing Principles

- The following design attributes/requirements are derived and carried over into the new system:
  - Control applications are partitioned onto separate controllers to prevent the introduction of new failures that could adversely impact the plant design basis
  - Functionally redundant control applications separated onto diverse plant power sources
  - Time Response requirements for each control application are established
  - Key Parameters are identified that must be provided to the operator
  - Designing controller applications for continued operation independent of the communication network or state of other controllers in the system
  - Establishing controller restart or shut down action requirements including I/O states designed for controller loss to revert to known or benign/safe state

Governing Design Principle Common Cause Failure (CCF)

- CCF of multiple SSCs is especially important to consider for digital I&C because the anticipated operational occurrences (AOO) and the analyses for postulated accidents (PA) are based in part on the ***failures*** and ***resulting malfunctions*** assumed for ***analog*** I&C
- However, digital implementations may introduce additional failures that have the potential to cause SSC malfunctions that may not have been considered for analog I&C. For example:
  1. Multiple SSCs are more commonly integrated into digital I&C equipment, either directly or through data communication interconnections than they were in analog I&C equipment
  2. The complexity of digital equipment can make a design defect more likely than for analog I&C
  3. Digital equipment has environmental sensitivities that were not as prevalent in analog I&C
- Therefore, for digital implementations it is important to confirm that those malfunctions and failures are still valid, or update the safety analysis to consider new malfunctions or failures

Governing Design Principle Common Cause Failure (CCF)

- Common Cause Failure is defined as:

  Concurrent failures (that is, multiple failures which occur over a time interval during which it is not plausible that the failures would be corrected) of multiple systems, structures or components (SSCs) that occur as a consequence of a single source (event or cause)

  - For example, a single controller failure that causes spurious repositioning of multiple valves results in a CCF

- Sources of CCF:

  1. A single random failure of a shared resource
  2. A single environmental disturbance (e.g., heat, EMI, etc.)
  3. A single design defect (e.g., a software design error, a requirements error, etc.)
  4. An operations or maintenance error

- The 7300 upgrade project will perform a CCF susceptibility analysis against all four CCF sources. Defensive measures that can ***prevent*** a CCF at each source will be applied, and if a CCF cannot be prevented at the source, then defensive measures will be applied to ***limit*** the effects of a CCF

CCF Source 1: Single Failure of a Shared Resource

- A single random failure of a shared resource is within the design basis of the facility
  - Consistent with SRP Section 7.7, “Control Systems,” the failure of any control system component or any auxiliary supporting system for control systems will not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the UFSAR
- The 7300 upgrade project will:
  1. Systematically assess the design to determine the likelihood of a CCF (of multiple controlled SSCs) due to a single failure of any shared resource (i.e., power supply, sensor, controller, control signal, output module, workstation, network, clock)
  2. If a CCF due to a single failure is not prevented, then a CCF coping analysis will be performed to determine if the plant level effect of the CCF (i.e., the CCF malfunction result) is already bounded by an existing Anticipated Operational Occurrence (AOO) described in the UFSAR
  3. If the plant level effect of any CCF due to a single failure is not bounded, then the preferred course is to modify the design so that the CCF result becomes bounded by an existing AOO
  4. If any plant level effects of a CCF due to a single failure are still not bounded by an existing AOO, then it is a malfunction with a different result and a License Amendment Request (LAR) will be initiated, assuming the CCF results meet design basis acceptance criteria

CCF Source 2: Single Environmental Disturbance

- A single environmental disturbance is within the design basis of the facility if the disturbance is caused by a single failure (e.g., loss of non-redundant HVAC)
- The 7300 upgrade project will:
  1. Confirm that Ovation equipment has been tested and demonstrates error-free performance for the worst-case environmental conditions to which it will be exposed (e.g. EMI, heat, fire etc.)
  2. Identify any single failures that can lead to adverse environmental conditions and a resulting control system CCF
  3. If a CCF due to a design basis environmental disturbance is not prevented, then a CCF coping analysis will be performed to determine if the plant level effect of the CCF (i.e., the CCF malfunction result) is already bounded by an existing AOO described in the UFSAR
  4. If the plant level effects of any CCFs due to a design basis environmental disturbance are not bounded, then the preferred course is to modify the design so that each CCF result becomes bounded by an existing AOO
  5. If any plant level effects of a CCF due to a design basis environmental disturbance are still not bounded by an existing AOO, then it is a malfunction with a different result and a License Amendment Request (LAR) will be initiated, assuming the CCF results meet design basis acceptance criteria

CCF Source 3: Single Design Defect

- A CCF due to a single design defect, including a software defect, is beyond the design basis of the facility
  - Consistent with SRP Section 7.7, "Control Systems," the control system is designed using a structured process similar to that applied to safety systems, but tailored to account for the lower safety significance. Therefore, consistent with IEEE-379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," a CCF due to a single design defect, including a software defect, is beyond the design basis of the facility
- The 7300 upgrade project will:
  1. Systematically assess the design to determine the likelihood of a CCF due to a single design defect (i.e. operating system, application software)
  2. If a CCF due to a single design defect is not prevented, then a CCF coping analysis will be performed to determine if the plant level effect of the CCF (i.e., the CCF result) is already bounded by:
     a) an existing AOO or Postulated Accident (PA) described in the UFSAR, or
     b) beyond design basis acceptance criteria
  3. If the plant level effects of any CCFs due to a single design defect are not bounded per point 2 above, then the design will be modified so that each CCF result becomes bounded

CCF Source 4: Operations or Maintenance Error

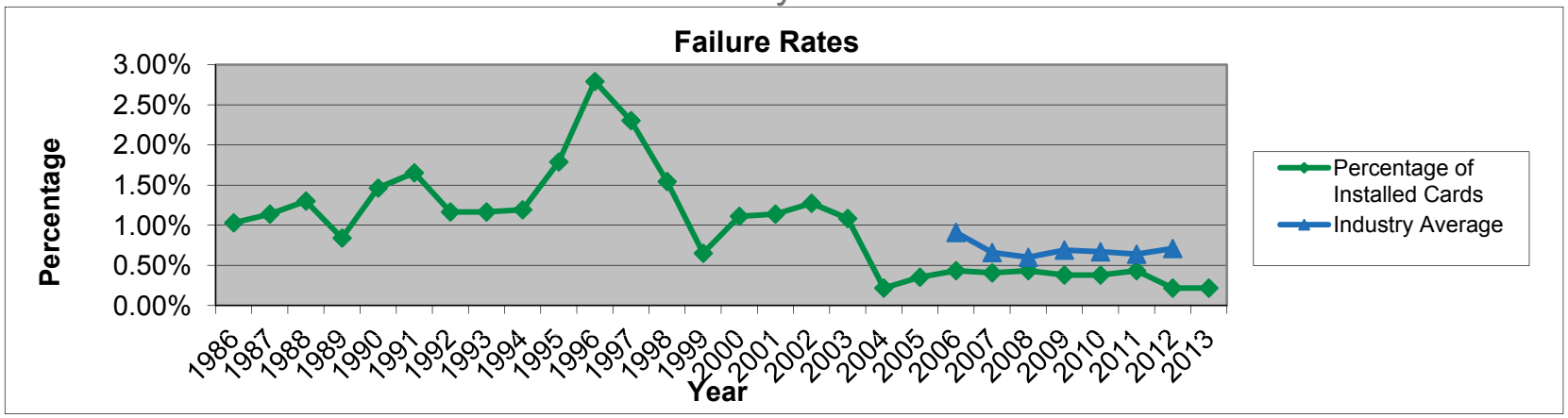
- A CCF due to an operations or maintenance error is preventable.
- The 7300 upgrade project will:
  1. Apply HFE protocols as delineated in NUREG 0700, Rev 2
  2. Apply a comprehensive training strategy for Operations, Maintenance and Engineering (included in the project plan)
  3. Modify the simulator in advance of installation to facilitate appropriate training of licensed operators

Using a comprehensive and systematic evaluation of the design, Exelon will address Single Point Vulnerabilities and potential sources of CCF to ensure that the use of the new digital equipment does not increase the likelihood of a malfunction and does not introduce new malfunctions that would create unanalyzed conditions that could jeopardize safety or reliability

Attachment 1 - Equipment Reliability Data

Context – Historical Equipment Reliability

- The 7300 system has exhibited performance, maintenance and reliability issues in the past
- In the late 90's and early 00's these reached unacceptable levels and a preemptive replacement strategies were undertaken to reduce the number of in-service failures (principally NLP cards) which have now been installed for roughly 15 years.
- The replacement strategy was effective in reducing the number of in-service failures but the cost of continual card replacements is exceptionally high, requires significant maintenance resources that are finite and does not address the inherent limitations of the systems architecture
- Though failure rate is currently low, it is expected to increase over time as components continue to age
- Given the large population of NSR circuit cards, even a modest failure rate of 0.5% translates to 22 in-service failures annually



Exelon Generation

7300 Circuit Card Reliability

- Historical data indicates that a typical card will fail between 6 and 14 years of service
- “In-kind” replacements are available but the limited performance history has been mixed – strong anecdotal evidence suggests that redesigned analog components are not as reliable as the cards they replace and will therefore fail more frequently
- Simply replacing the circuit cards, while simple in concept, fails to capitalize on opportunities to improve fault tolerance, improve equipment reliability and reduce initiating events